

REMARKS

This Amendment is in response to the Office Action dated July 26, 2005. Because this response is mailed on October 26, 2005, with a Request for Continued Examination, the Amendment is timely filed.

I. Status of the Amendments

Prior to this amendment, claims 1-10 and 13-17 were pending. By this amendment, claim 6 has been canceled without prejudice to refile, and claims 1-5, 8-10, 16 and 17 have been amended. Consequently, claims 1-5, 7-10 and 13-17 are presently pending.

Because applicant previously paid for 4 independent claims and 20 total claims, no additional fee is due.

II. Response to July 26 Office Action

In the July 26 Office Action, claims 1-9, 16 and 17 were rejected as being allegedly anticipated under 35 U.S.C. §102(b) over Graunke et al. (U.S. Pat. No. 5,991,399), and claims 10 and 13-15 as being allegedly unpatentable under 35 U.S.C. §103 over Graunke et al. in view of Alcorn (U.S. Pat. No. 5,643,086). Applicant has amended the claims, and has the following comments in response.

Claim 1, as amended, recites a method of providing control code for operating a gaming device initiating operation of the gaming device. The method includes obtaining gaming device operational code reversibly encrypted with a first private key, the operational code comprising at least one of audio or video data used during play of a game on the device. The method also includes providing said encrypted operational code to said gaming device, and providing said first private key to said gaming device separately from said encrypted operational code. The method further includes decrypting said encrypted operational code using said first private key to recover said code, storing said decrypted operational code at

said gaming device, and utilizing said decrypted operational code to control at least some audio or video aspect of the operation of said gaming device during operation of said gaming device by said player.

Thus, in particular, claim 1 recites that the first private key, which is used to decrypt the encrypted operational code, is provided to the gaming device separately from the encrypted code.

By contrast, Graunke et al. uniformly states that the allegedly corresponding key that is used to decrypt the allegedly corresponding reversibly encrypted operational code is provided to the allegedly corresponding gaming device with the allegedly corresponding encrypted operational code. Graunke et al. states, in the summary of the invention, that the “tamper resistant key module” includes the generated private key and the encrypted predetermined data to be decrypted using the private key. See, col. 3:11-20. Moreover, Graunke et al. specifically teaches away from providing the key separately from the data, stating that the key should not be nakedly transmitted (see, e.g., col. 4:2) or “pre-loaded” into the gaming device (see, e.g., col. 2:62-64, col. 3:61-64). Thus, Graunke et al. not only does not disclose the subject matter of the limitation noted above, it teaches and suggests away from such subject matter.

Consequently, Graunke et al. does not disclose each and every limitation of claim 1, as amended. Because Graunke et al. does not disclose each and every limitation of claim 1, it does not anticipate claim 1. Therefore, the rejection of claim 1 should be withdrawn.

Similar to claim 1, claim 5 recites, in part, providing said encrypted operating data to said gaming device, providing said first private key to said gaming device separately from said encrypted operational code, and decrypting said encrypted operating data with said decryption device using said first key to recover said operating data. Given the similarity between these limitations and those noted above relative to claim 1, applicant submits that the arguments provided above apply with equal force to claim 5. Therefore, the rejection of claim 5 should also be withdrawn.

Claim 16 recites, in part, encrypting a first portion of a set of operating data with a first private key and a second portion of said set of operating data with a second private key, said operating data including at least one of audio or video data used during play of a game

by a player on the device, providing said encrypted operating data to said gaming device, providing one of said first or second private keys to said gaming device separately from said encrypted operating data, and utilizing said provided private key to decrypt said first or second portion of said set of encrypted operating data. Here as well, given the similarity between these limitations and those noted above relative to claim 1, applicant submits that the arguments provided above apply with equal force to claim 16. Therefore, the rejection of claim 16 should also be withdrawn.

As to the rejections of claims 2-4, 7-9, and 17, applicants note that claims 1, 5 and 16 are not anticipated by Graunke et al., for the reasons provided above, and that claims 2-4, 7-9, and 17 depend from claims 1, 5 or 16. Therefore, claims 2-4, 7-9, and 17 should also be allowable at least for the reason that they depend from claims 1, 5 or 16. Consequently, the rejections of claims 2-4, 7-9 and 16 should be withdrawn.

As to the rejection of claim 10, the rejection is premised on the applicability of Graunke et al., Alcorn being relied upon for teaching "the use of RAM in a casino wagering system." Thus, applicant notes that claim 10 recites, in pertinent part, (i) a memory device for storing operating data reversibly encrypted in a symmetrical encryption process, said operating data including at least one of audio or video data used during play of a game on the device; (ii) a secure access module including a stored private decryption key for decrypting data encrypted in a symmetrical encryption process to recover said operating data, said stored private decryption key provided to the secure access module separately from said reversibly encrypted operating data; and (iii) control code effecting location of said private decryption key and use of said key to decrypt said operating data. Thus, similar to claims 1, 5, and 16, the private decryption key used to decrypt the encrypted operating data is provided to the secure access module separately from said reversibly encrypted operating data. Consequently, applicant submits that the arguments raised above apply with equal force to the rejection of claim 10, which rejection should be withdrawn.

As to the rejections of claims 13-15, claims 13-15 should also be allowable at least for the reason that they depend from claim 10. Consequently, the rejections of claims 13-15 should be withdrawn.

If there is any matter that the Examiner would like to discuss, the Examiner is invited to contact the undersigned representative at the telephone number set forth below. In any event, the Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 13-2855, under Order No. 29757/P-227. A duplicate copy of this paper is enclosed.

Dated: October 26, 2005

Respectfully submitted,

By 

Paul C. Craane

Registration No.: 38,851

MARSHALL, GERSTEIN & BORUN LLP

233 S. Wacker Drive, Suite 6300

Sears Tower

Chicago, Illinois 60606-6357

(312) 474-6300

Attorney for Applicant